



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/506,830	02/18/2000	Daniel I Flitcroft	032668-006	9055

21839 7590 10/06/2003

BURNS DOANE SWECKER & MATHIS L L P  
POST OFFICE BOX 1404  
ALEXANDRIA, VA 22313-1404

EXAMINER

GRAHAM, CLEMENT B

ART UNIT PAPER NUMBER

3628

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/506,830

Applicant(s)

FLITCROFT ET AL.

Examiner

Clement B Graham

Art Unit

3628

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 May 2003.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-10, 12-16, 18, 20-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10, 12-16, 18, 20-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 15.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. In view of the Appeal brief filed on 5/6/03, PROSECUTION IS HEREBY REOPENED. in view of new grounds of rejection set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. Claims 1-10, 12-16, 18, 20-28 remained.

**Claim Rejections - 35 USC § 103**

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter

Art Unit: 3628

pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-10, 12-16, 18, 20-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Franklin et al (Hereinafter Franklin U.S. Patent No. 5883810 in view of Cohen U.S. Patent 642462.

As per claims 1-3, Franklin discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the

Art Unit: 3628

online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin). Franklin also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries. (See column 6 lines 50-65 of Franklin). Franklin also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15) and the transaction number can be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction

Art Unit: 3628

number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 50-55).

Franklin fails to teach limited use credit card number that is not yet activated.

However Cohen discloses corporation can issue customized credit cards, or obtain customized credit cards from a credit card company, which can serve certain limited uses, functions or so forth. This card can be customized in any of numerous ways. For example, the customized card could be set to be valid for a certain limited number of dates or until a certain date. For example, if an employee is going on a business trip for two days (or some other amount of time), the card could be set to be valid on only those two days. Thus, the employee is authorized to use the card for charges on only that time that the employee is away on the business trip, but not for any other time. Thus, in accordance with these embodiments, the card can have a user customized range of dates or series of dates.(see column 7 lines 30-65) and customization (and activation) of the card or a specific credit card number can be in any of the ways known in the art for example, the user can call the credit card company and, once his or her identity has been verified, can direct the credit card company to customize the card (or a specific credit card or credit card number on the account) in the manner desired and/or to activate that specific credit card or credit card number and the user could be required to call from his or her home phone, with the phone number being verified at the credit card company using "Caller ID".(see column 12 lines 35-65) and Customized credit and debit cards for issuance by a person or main cardholder, the cards being limited to use in transactions at selected vendors only. Thus, for example, a parent or corporation can

Art Unit: 3628

issue a customized card to a person or group, wherein the card is only valid for use at restaurants, airlines, hotels, certain stores, or so forth.(Note abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin to include limited use credit card number that is not yet activated taught by Cohen in order to prevent credit card fraud and an unscrupulous individual obtains a copy of a person's credit card information, and then uses that information to fraudulently charge purchases to the person's card until the theft is noticed and further use of the card is blocked. In addition to being a considerable problem for the card companies themselves, this illegal practice causes inconvenience and annoyance for the innocent user whose card has somehow been compromised.

As per claim 4, Franklin discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN("i. e, identify user"), the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations. (See column 7 lines 5-30 of Franklin). Franklin also discloses for added security, the transaction number can

Art Unit: 3628

be linked to extra transaction information to ensure that the number is only used for one specific transaction. For instance, the issuing institution might tie the transaction number to a specific purchase amount and a particular merchant ID. The issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 50-55 of Franklin

et al). Franklin does not explicitly teach requesting validation of a limited use credit card for a merchant as identified by a merchant identification number.

However Cohen discloses user can customized the limited use card(see column 5 lines 20-25) and Internet, he or she accesses one of his or her disposable credit cards or credit card numbers. As noted above, this could be accomplished by dialing into the credit card company, by removing one of a series of disposable cards from the user's monthly statement, or so forth. To effect the transaction over the Internet, the user transmits his or her credit card information to the vendor. That vendor then verifies the transaction and obtains an authorization code from the credit card company authorizing the purchase, as is currently standard practice with credit card transactions. To insure the integrity of the system, the vendor is required to verify the code immediately upon receipt. This prevents undue time from elapsing, which is undesirable from a security standpoint.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to that the teachings of Franklin can be modified to include Cohen in order to validate a limited use credit card for a merchant as identified by a merchant identification number.



Art Unit: 3628

As per claim 5, Franklin discloses during the payment authorization phase, the merchant submits the transaction number over the conventional payment network to the issuing bank for approval. The issuing bank identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank uses the transaction number to retrieve the data record linking the transaction number to a customer account number. The issuing bank then swaps the customer account number for the transaction number and processes the authorization request using its conventional processing system. After the processing, the issuing bank substitutes the transaction number back for the customer account number and returns the authorization reply to the merchant under the transaction number. In this manner, only the issuing bank is aware that the transaction number is a proxy for the customer account number. The merchant need not be aware that the transaction number is not a true customer account number, but simply handles the number as it would any other card number. (See column 5 of Franklin). Franklin also discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth. (See column 2 lines 30-40 of Franklin). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin). Franklin fails to teach deactivating the limited use credit card number by the card issuer when a triggered condition is present. However Cohen discloses after a one time use, the credit card number is deactivated by the issuing credit card company. (See column 5 lines 40-42).

Art Unit: 3628

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made that the teachings of Franklin to include deactivating the limited use credit card number by the card issuer when a triggered condition is present which is taught by Cohen in order to prevent credit card fraud or misuse.

As per claim 6-7, Franklin discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth.(See column 2 lines 30-40 of Franklin). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin). Franklin fails to teach communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step or revalidating the use credit card number with associated limited use properties .

However Cohen discloses for example, it could be valid for a specific day or series of date in March (for a first business trip), become deactivated once that trip is over, can be reactivated for a specific day or dates in June (for a second business trip), be deactivated once that trip is over, and so forth. It could also be valid for a specific predetermined amount of time. For example, it could be valid for any one week period, beginning from when the user or subuser uses first (see column 7 lines 50-60).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin to include communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step or revalidating the use

Art Unit: 3628

credit card number with associated limited use properties in order to prevent credit card fraud before a user credit card can be comprised.

As per claim 8-10, Franklin discloses during the payment authorization phase, the merchant submits the transaction number over the conventional payment network to the issuing bank for approval. The issuing bank identifies the number as a transaction number, as opposed to a real customer account number. The issuing bank uses the transaction number to retrieve the data record linking the transaction number to a customer account number. The issuing bank then swaps the customer account number for the transaction number and processes the authorization request using its conventional processing system. After the processing, the issuing bank substitutes the transaction number back for the customer account number and returns the authorization reply to the merchant under the transaction number. In this manner, only the issuing bank is aware that the transaction number is a proxy for the customer account number. The merchant need not be aware that the transaction number is not a true customer account number, but simply handles the number as it would any other card number. (See column 5 of Franklin). Franklin also discloses the issuing institution can use the existing processing system to check account information spending limits, and so forth. (See column 2 lines 30-40 of Franklin). Franklin also discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 line 50 of Franklin). Franklin fails to teach deactivating the limited use credit card number by the card issuer when a triggered condition is present.

Art Unit: 3628

However Cohen discloses after a one time use, the credit card number is deactivated by the issuing credit card company. (See column 5 lines 40-42).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made that the teachings of Franklin to include deactivating the limited use credit card number by the card issuer when a triggered condition is present which is taught by Cohen in order to prevent credit card fraud or misuse.

As per claim 12, Franklin fails to teach transmitting a signal to merchant denying authorization of the card number if the credit card number has been deactivated. However Cohen discloses credit discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin). That vendor then verifies the transaction and obtains an authorization code from the credit card company authorizing the purchase, as is currently standard practice with credit card transactions. To insure the integrity of the system, the vendor is required to verify the code immediately upon receipt. This prevents undue time from elapsing, which is undesirable from a security standpoint. Upon receiving the request for verification, the credit card company notes the identity of the vendor, authorizes the transaction (if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor. At the same time, the credit card company also deactivates the credit card number from any further future use. Thus, if a thief intercepts the credit card information en route, when the thief later attempts to take that information and to use it in an illegal transaction, the transaction will be declined since the number has already been deactivated. After the number has legitimately been

Art Unit: 3628

used once by the lawful owner, it no longer has any continuing validity. (See column 5 lines 30-55).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin to include transmitting a signal to merchant denying authorization of the card number if the credit card number has been deactivated taught by Cohen in order to prevent fraud or illegal transaction and to enforce a restriction associated with the transaction number.

As per claim 13-14, Franklin discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase the issuing

Art Unit: 3628

institution recognizes the number as a transaction number for an online commerce card.

The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40).

As per claim 15, Franklin fails to teach declining authorization of the transaction based on the results of the authorization determining step.

However Cohen discloses credit discloses the issuing institution might further impose a short expiration term on the transaction number so that the number becomes invalid after the expiration term lapses. (See column 2 lines 30-50 of Franklin). That vendor then verifies the transaction and obtains an authorization code from the credit card company authorizing the purchase, as is currently standard practice with credit card transactions. To insure the integrity of the system, the vendor is required to verify the code immediately upon receipt. This prevents undue time from elapsing, which is undesirable from a security standpoint. Upon receiving the request for verification, the credit card company notes the identity of the vendor, authorizes the transaction if the credit card number is valid and the purchaser has sufficient funds available), and forwards the authorization code to the vendor. At the same time, the credit card

Art Unit: 3628

company also deactivates the credit card number from any further future use. Thus, if a thief intercepts the credit card information en route, when the thief later attempts to take that information and to use it in an illegal transaction, the transaction will be declined since the number has already been deactivated. After the number has legitimately been used once by the lawful owner, it no longer has any continuing validity. (See column 5 lines 30-55).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin to include declining authorization of the transaction based on the results of the authorization determining step taught by Cohen in order to prevent fraud or illegal transaction and to enforce a restriction associated with the transaction number, system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40).

As per claims 16, Franklin discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number

Art Unit: 3628

and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth and Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin). Franklin also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries.(See column 6 lines 50-65 of Franklin). Franklin also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for



Art Unit: 3628

certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin).

As per claims 18, 20-21, Franklin discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online

Art Unit: 3628

commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth. Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin). Franklin also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries. (See column 6 lines 50-65 of Franklin). Franklin also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15) and customer record for customer stored in customer database and (see column 9 lines 5-40) and The merchant has a computing unit implemented in the form of a computer server, although other implementations are possible. The bank has a computing center shown as a mainframe computer.

Art Unit: 3628

However, the bank computing center may be implemented in other forms, such as a minicomputer, a PC server, a networked set of computers, and the like.(see column3 lines 50-55).

As per claims 22-28, Franklin discloses an online commerce card is issued electronically to a customer by an issuing institution, such as a bank or third party certifying authority. The issued card is assigned a permanent customer account number that is maintained on behalf of the customer by the issuing institution. The customer account number is not given to the customer to remove the risk of that number being lost or stolen. When the customer desires to conduct an online transaction, the customer sends a request to the issuing institution to issue a transaction number for a single transaction. The issuing institution generates a temporary transaction number and associates it with the permanent account number in a data record. The customer receives the transaction number and submits that number to the merchant as a proxy for the customer account number during the transaction. The transaction number looks like a real card number (i.e., it has the same format and number of digits as a regular credit card). To the merchant, the transaction number is treated the same as any regular credit card number. The merchant handles the proxy transaction number according to traditional protocols, including seeking authorization from the issuing institution to honor the card number. During the authorization phase, the issuing institution recognizes the number as a transaction number for an online commerce card. The issuing institution references the customer account number associated with the online commerce card, using the transaction number as an index to the appropriate data record, and processes the authorization request using the card's true customer

Art Unit: 3628

account number. In this manner, the issuing institution can use its existing processing system to check account information, spending limits, and so forth.

Once the authorization request is processed, the issuing institution once again exchanges the card's transaction number for the card's customer account number and sends an authorization reply back to the merchant under the transaction number. (See column 2 lines 5-40 of Franklin). Franklin also discloses that a PIN and software stored on a floppy disk and mailed to the customer using conventional postal carries. (See column 6 lines 50-65 of Franklin). Franklin also discloses the customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations (See column 7 lines 5-15 of Franklin). Franklin fails to teach communicating with a limited use card number card issuer to activate the limited use credit card number before it can be used in a transaction wherein the properties of said activation are defined by the user and the card is only activated for user defined limited uses. However Cohen discloses for example, the user can call the credit card company and, once his or her identity has been verified, can direct the credit card company to customize the card (or a specific credit card or credit card number on the account) in the

Art Unit: 3628

manner desired and/or to activate that specific credit card or credit card number and the user could be required to call from his or her home phone, with the phone number being verified at the credit card company using "Caller ID".(see column 12lines 35-65).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Franklin to include communicating with a limited use card number card issuer to activate the limited use credit card number before it can be used in a transaction wherein the properties of said activation are defined by the user and the card is only activated for user defined limited uses taught by Cohen in order to prevent credit card fraud and an unscrupulous individual obtains a copy of a person's credit card information, and then uses that information to fraudulently charge purchases to the person's card until the theft is noticed and further use of the card is blocked. In addition to being a considerable problem for the card companies themselves, this illegal practice causes inconvenience and annoyance for the innocent user whose card has somehow been compromised.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clement B Graham whose telephone number is 703-305-1874. The examiner can normally be reached on 7am to 5pm.

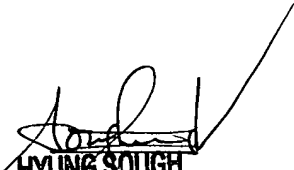
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on 703-305-0505. The fax phone numbers for the organization where this application or proceeding is assigned are 703-305-0040 for regular communications and 703-305-0040 for After Final communications.

Art Unit: 3628

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

CG

September 29, 2003

  
HYUNG SOUGH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600